La présente invention est relative aux dispositifs pour la génération de signaux aléatoires.

Elle trouve avantageusement, mais non limitativement, application aux dispositifs pour la génération de signaux aléatoires du type à circuit(s) logique(s).

Un but général de l'invention est de proposer un dispositif permettant la génération de signaux aléatoires de qualité.

On connaît déjà de nombreux dispositifs à circuits logiques présentés comme permettant la génération de signaux aléatoires (combinaison d'horloges asynchrones, utilisation du positionnement à la mise sous tension d'un plan mémoire). Le caractère aléatoire de tels dispositifs peut-être pris en défaut sous certaines conditions, ce qui les rend impropres pour de nombreuses applications où la qualité de l'aléa est primordiale tel que le chiffrement des données.

Lorsqu'un aléa de qualité est désiré, les concepteurs de circuits électroniques ont habituellement recours à des systèmes analogiques (tel que l'amplification d'un bruit de fond). Ces solutions ne sont pas intégrables dans des circuits logiques et notamment dans des ASICs ou FPGAs. Il en résulte une perte d'intégration, puisqu'il est nécessaire d'utiliser un dispositif spécifique afin de réaliser la fonction requise.

Un autre but de l'invention est de proposer une solution apte à être réalisée avec des circuits logiques.

On sait que les bruits électroniques sont classés en deux catégories principales : le bruit thermique et le bruit de grenaille (également souvent désigné par "popcorn noise", ou "bruit popcorn", par l'homme du métier pour décrire les instabilités du niveau moyen d'un signal à variation rapide).

L'invention propose quant à elle de tirer partie des bruits d'origine thermique et de leur combinaison avec les bruits de jonction des semi-conducteurs.

Elle propose en particulier un dispositif pour la génération d'un signal aléatoire, caractérisé en ce qu'il comprend un circuit électronique à état transitoire, ainsi que des moyens aptes à commander l'activité et/ou

l'arrêt dudit circuit, afin de générer un signal aléatoire sur la sortie de celui-ci.

Un tel circuit à état transitoire, selon qu'il est en activité ou que son activité est arrêtée, s'échauffe ou se refroidit. Son échauffement génère en sortie un signal aléatoire.

Le circuit comporte avantageusement, mais non limitativement, des moyens logiques à semi-conducteur(s).

Notamment, dans un mode de réalisation préféré, le dispositif comporte un circuit oscillateur à moyens de type semi-conducteur(s) et des moyens aptes à commander l'activité et/ou l'arrêt dudit circuit.

Avec un tel oscillateur, le bruit d'origine thermique et le bruit de jonction des semiconducteurs s'amplifient l'un, l'autre pendant une phase d'échauffement, notamment au démarrage du dispositif. La vitesse des porteurs aux jonctions dépend de la température ; celle-ci augmente lors des opérations de transfert des porteurs. Il y a une « auto – amplification » de l'instabilité jusqu'à stabilisation thermique du dispositif (c'est-à-dire la chaleur produite est égale à la chaleur évacuée). Le phénomène d'instabilité n'existe ainsi que durant une période très courte (durée nécessaire pour que la jonction passe de la température ambiante à une température stable). Cette durée varie de la centaine de micro-seconde à au plus la milli-seconde pour les circuits expérimentés (en particulier des circuits CMOS en 0,8 micron). Ce paramètre est propre à une technologie donnée.

Avantageusement encore, la sortie du circuit oscillateur est bouclée sur l'entrée de celui-ci.

Le bouclage du circuit sur lui-même auto amplifie les phénomènes d'instabilité sur la sortie non contrôlée du circuit. Le circuit utilise ainsi sa propre instabilité afin de l'amplifier (et de l'entretenir le plus longtemps possible).

Dans un mode de réalisation préféré, le circuit oscillateur comporte des moyens formant inverseur qui inversent sur sa sortie le signal présent à son entrée, ainsi qu'une boucle entre son entrée et sa sortie.

Notamment, des moyens aptes à commander le fonctionnement ou l'arrêt du circuit oscillateur peuvent comporter des moyens formant interrupteurs disposés dans la boucle entre la sortie des moyens formant inverseur et la sortie du circuit oscillateur.

Les moyens formant inverseurs peuvent comporter une pluralité d'inverseurs en nombre impair.

Par ailleurs, le phénomène utilisé ayant un caractère éphémère, on couple, afin d'obtenir un flux continu, au moins deux dispositifs, l'un fournissant l'instabilité pendant que l'autre refroidi.

Ainsi, l'invention a également pour objet un dispositif à circuit(s) logique(s) pour la génération d'un signal aléatoire, caractérisé en ce que pour générer ledit signal aléatoire de façon continue, il comporte plusieurs dispositifs, des moyens pour commander successivement de façon alternée l'activité, puis l'arrêt des circuits à état transitoire de chacun des dispositifs, ainsi que des moyens pour combiner les sorties des différents dispositifs.

Avantageusement, les moyens de combinaison mettent en œuvre sur les sorties des différents dispositifs une combinaison de type OU EXCLUSIF.

De préférence, les moyens de commande comportent au moins un compteur qui reçoit en entrée le signal en sortie de moyens combinant les sorties des différents dispositifs, ainsi que des moyens pour commander l'activité et/ou l'arrêt des moyens de type à semi-conducteur(s) desdits dispositifs en fonction du décompte dudit compteur.

Comme on l'aura compris, les dispositifs proposés par l'invention sont avantageusement intégrés dans un circuit intégré spécifique ou dans un circuit intégré programmable (ASIC ou FPGA).

D'autres caractéristiques et avantages de l'invention ressortiront encore de la description qui suit, laquelle est purement illustrative et non limitative et doit être lue en regard des dessins annexés sur lesquels :

- la figure 1 est un schéma de principe d'un dispositif à circuit logique conforme à un mode de réalisation possible de l'invention ;

- la figure 2 est un schéma d'un dispositif à flux continu conforme à un mode de réalisation possible de l'invention ;

- la figure 3 est un schéma d'un dispositif analogique illustrant un autre mode de réalisation possible de l'invention.

Le circuit 11 qui illustre un exemple de réalisation possible de l'invention comprend un inverseur 111 - ou une série d'inverseurs en nombre impair - bouclé sur lui-même à travers une porte logique 112.

Cette porte, qui constitue un moyen formant interrupteur qui autorise ou non le re-bouclage du signal, est commandée par un signal externe 12.

Tant que le circuit 11 n'est pas stabilisé thermiquement, sa sortie 13 présente un caractère aléatoire (en fréquence essentiellement) lorsque la commande 12 autorise le bouclage. Ce caractère aléatoire est fortement présent et exploitable jusqu'à la stabilisation thermique du circuit.

Le mode de réalisation illustré sur la figure 2 permet quant à lui de générer un signal aléatoire sans discontinuité.

Le dispositif, référencé par 14, qui est représenté sur cette figure 2, comporte plusieurs circuits du type du circuit de la figure 1, en l'occurrence deux, référencés par 11a et 11b. Le nombre de circuits est ici réduit pour la simplification de l'exposé, mais peut être bien entendu plus important. Notamment, les inventeurs ont testé des dispositifs comportant jusqu'à cinq circuits du type de celui de la figure 1.

Les moyens qui commandent les circuits 11a, 11b sont tels qu'un seul de ces circuits n'est exploité à la fois.

Les sorties 13a, 13b sont combinées dans des moyens 20 pour générer un seul signal de sortie (sortie 15).

Les moyens 20 qui assurent la combinaison des sorties 13a, 13b sont constitués par un circuit XOR (OU EXCLUSIF), ce qui permet de s'affranchir de l'état 1 ou 0 du circuit stable.

Egalement, une sortie combinée alimente un compteur 21 qui réalise un décompte suivant un modulo choisi. Ce modulo est choisi aussi grand que possible, sans néanmoins être trop important afin que le temps de comptage pour l'atteindre soit toujours inférieur au temps de stabilisation thermique.

En l'occurrence, sur le schéma de la figure 2, le dispositif 21 intègre à la fois des moyens de comptage et un circuit XOR de combinaison en amont de ces moyens.

La sortie 21a de bit de poids fort du compteur 21 est utilisée pour commander les portes logiques des circuits 11a, 11b. Ce bit 21a est envoyé directement à l'un des circuits et est inversé avant d'être envoyé sur l'autre. En l'occurrence, le signal 21a constitue directement le signal 12a qui commande le circuit 11a. Il est inversé à travers un inverseur 22 pour constituer le signal 12b qui constitue le circuit 11b.

L'invention a été ici décrite dans le cas d'un circuit spécifique à oscillateur logique, mais s'applique de façon plus générale à tout dispositif comportant des moyens à semi-conducteur(s) et de façon encore plus générale à tout dispositif comportant un circuit électronique à état transitoire. De tels moyens présentent en effet lors d'un échauffement ou d'un refroidissement (par lui-même ou par un autre moyen, par exemple des circuits proches) une instabilité, laquelle se manifeste par une variation aléatoire de la vitesse de combinaisons-recombinaisons des porteurs ce qui influence de nombreux paramètres : temps de propagation, temps de montée et de descente des signaux, fan-out etc. Et cette activité de combinaisons-recombinaisons produit de la chaleur.

Notamment, l'invention peut également trouver application avec des structures à circuits analogiques.

Une structure en ce sens est illustrée sur la figure 3, sur laquelle on a représenté un circuit analogique qui comporte : un amplificateur différentiel 30 et deux ponts diviseurs de tension 31, 32 identiques dont les sorties sont injectées sur respectivement l'une et l'autre des deux entrées de l'amplificateur 30. L'alimentation de ces deux ponts diviseurs 31, 32 est commandée par un interrupteur 33.

Durant la phase d'échauffement des résistances des ponts diviseurs 31, 32, il existe une différence de tension entres les sorties des deux ponts diviseurs, qui est un signal aléatoire qu'il est possible d'exploiter grâce à l'amplificateur différentiel 30.

Les solutions à circuits logiques de type à semi-conducteur(s) sont néanmoins préférés.

Le dispositif est alors avantageusement intégré sur un circuit FPGA ou un ASIC. Les inventeurs ont notamment testé l'invention avec une réalisation sur un ACTEL 1010.

Dans le cas d'un ASIC, le ou les dispositifs de génération d'aléa sont avantageusement disposés dans des zones ayant des activités électriques les moins synchrones possibles.